Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 March 2025

Vulnerabilities

Cisco fixed command injection and DoS flaws in Nexus switches

Security Affairs - 28 February 2025 12:59

Cisco addressed command injection and denial-of-service (DoS) vulnerabilities in some models of its Nexus switches. Cisco released security updates to address command injection and DoS vulnerabilities in Nexus switches, including a high-severity flaw. The most severe issue, tracked as CVE-2025-20111 (CVSS Score of 7.4), resides in the health monitoring diagnostics of Cisco Nexus 3000 Series […]

RDP: a Double-Edged Sword for IT Teams – Essential Yet Exploitable

The Hacker News - 28 February 2025 20:53

Remote Desktop Protocol (RDP) is an amazing technology developed by Microsoft that lets you access and control another computer over a network. It's like having your office computer with you wherever you go. For businesses, this means IT staff can manage systems remotely, and employees can work from home or anywhere, making RDP a true game-changer in today's work environment.

Amnesty Reveals Cellebrite Zero-Day Android Exploit on Serbian Student Activist

SecurityWeek - 28 February 2025 21:20

Amnesty International publishes technical details on zero-day vulnerabilities exploited by Cellebrite's mobile forensic tools to spy on a Serbian student activist.

Threat actors and malware

Ransomware gangs exploit Paragon Partition Manager bug in BYOVD attacks

BleepingComputer - 01 March 2025 11:17

Microsoft had discovered five Paragon Partition Manager BioNTdrv.sys driver flaws, with one used by ransomware gangs in zero-day attacks to gain SYSTEM privileges in Windows. […]

US Cyber Command reportedly pauses cyberattacks on Russia

The Register - 03 March 2025 04:31

PLUS: Phishing suspects used fishing gear as alibi; Apple's 'Find My' can track PCs and Androids; and more Infosec In Brief US Defense Secretary Pete Hegseth has reportedly ordered US Cyber Command to pause offensive operations against Russia, as the USA's Cybersecurity and Infrastructure Security Agency (CISA) has denied any change in its posture....

Ransomware Group Takes Credit for Lee Enterprises Attack

SecurityWeek - 28 February 2025 12:43

The Qilin ransomware gang claims to have stolen 350 Gb of files from Lee Enterprises in the attack that caused newspaper disruptions.